

Further improvements on the Feng-Rao bound for dual codes

Olav Geil^{*1} and Stefano Martin^{†1,2}

¹Department of Mathematical Sciences, Aalborg University

²Engineering Software Institute, East China Normal University

May 7, 2013

Abstract

Salazar, Dunn and Graham in [15] presented an improved Feng-Rao bound for the minimum distance of dual codes. In this work we take the improvement a step further. Both the original bound by Salazar et. al., as well as our improvement are lifted so that they deal with generalized Hamming weights. We also demonstrate the advantage of working with one-way well-behaving pairs rather than weakly well-behaving or well-behaving pairs.

Keywords: Advisory bound, affine variety code, Feng-Rao bound, generalized Hamming weight, minimum distance, well-behaving pair.

MSC: 94B65, 94B27, 94B05.

1 Introduction

The celebrated Feng-Rao bound for the minimum distance of dual codes [2, 3] was originally presented in a language close to that of affine variety codes [4]. A more general result was derived by formulating the bound at the level of general linear codes [14, 13, 12, 6]. Among the general linear code formulations the weakest version uses one basis for \mathbb{F}_q^n and the concept of *well-behaving pairs* (WB). The stronger versions use two or even three bases and the concept of *weakly well-behaving* (WWB) or even *one-way well-behaving* (OWB). The strong linear code formulation is the most general of all versions of the Feng-Rao bound in the sense that all other formulations, including the order bound [8], can be viewed as corollaries to it.

In [15] Salazar, Dunn and Graham presented a clever improvement to the Feng-Rao bound for the minimum distance of dual codes which they name *the advisory bound* [15, Def. 40]. Their exposition uses a language close to that of

^{*}olav@math.aau.dk

[†]stefano@math.aau.dk

Feng and Rao's original papers. In the present paper we start by giving a general linear code enhancement of their bound and we lift it to deal with generalized Hamming weights improving upon the usual Feng-Rao bound for generalized Hamming weights of dual codes [7, 6]. We remind the reader that generalized Hamming weights among other things are relevant for the analysis of wiretap channels of type II [16, 11] and secret sharing schemes based on error correcting codes [9]. Our proof demonstrates that the advisory bound is a consequence of a lemma from which further improvements can be derived. These improvements are investigated in detail and are formulated in a separate bound. The new bound is then lifted to deal with generalized Hamming weights. Our exposition involves as a main ingredient a relaxation of the concept of OWB.

The paper [15] describes two families of affine variety codes for which the advisory bound is sometimes strictly better than the Feng-Rao bound. The first family [15, Sec. 3.1] is related to a curve over \mathbb{F}_8 . The second family [15, Sec. 3.2] relates to a surface over \mathbb{F}_4 . In Section 4 we shall give a thorough treatment of the curve from [15, Sec. 3.1] and a related curve over \mathbb{F}_{27} . As it shall be demonstrated for these curves sometimes the new bound produces much better results than the advisory bound. Also it is demonstrated for the first time in the literature that the Feng-Rao bound equipped with OWB can sometimes be much better than the same bound equipped with WWB. We do not treat the surface from [15, Sec. 3.2] in the present paper. This is due to the fact that it is more natural to treat the corresponding quotient ring as an order domain with weights in \mathbb{N}_0^2 [5, 1]. Doing so, one finds much better code parameters by applying the usual Feng-Rao bound than what was produced by the advisory bound in [15, Sec. 3.2]. It is beyond the scope of the present paper to give the details.

2 Enhancements of the advisory bound

To explain better what is the essence of Salazar, Dunn, and Graham's method, below we explain it at the level of general linear codes. We also extend their method to deal with generalized Hamming weights.

Let n be a positive integer and q a prime power. Throughout this and the following section we consider a fixed ordered triple $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ where $\mathcal{U} = \{\vec{u}_1, \dots, \vec{u}_n\}$, $\mathcal{V} = \{\vec{v}_1, \dots, \vec{v}_n\}$, and $\mathcal{W} = \{\vec{w}_1, \dots, \vec{w}_n\}$ are three (possibly different) bases for \mathbb{F}_q^n as a vector space over \mathbb{F}_q . By \mathcal{I} we shall always mean the set $\{1, \dots, n\}$.

Definition 1. Let the function $\bar{\rho}_{\mathcal{W}} : \mathbb{F}_q^n \rightarrow \{0, 1, \dots, n\}$ be given as follows. For $\vec{c} \neq \vec{0}$ we let $\bar{\rho}_{\mathcal{W}}(\vec{c}) = i$ if $\vec{c} \in \text{Span}\{\vec{w}_1, \dots, \vec{w}_i\} \setminus \text{Span}\{\vec{w}_1, \dots, \vec{w}_{i-1}\}$. Here, we used the notion $\text{Span}\emptyset = \{\vec{0}\}$. Finally, we let $\bar{\rho}_{\mathcal{W}}(\vec{0}) = 0$.

The following two concepts play a crucial role in our exposition.

Definition 2. The component wise product of two vectors \vec{u} and \vec{v} in \mathbb{F}_q^n is defined by $(u_1, \dots, u_n) * (v_1, \dots, v_n) = (u_1 v_1, \dots, u_n v_n)$.

Definition 3. Let an ordered triple of bases $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ be given. We define $m : \mathbb{F}_q^n \setminus \{\vec{0}\} \rightarrow \mathcal{I}$ by $m(\vec{c}) = l$ if l is the smallest number in \mathcal{I} for which $\vec{c} \cdot \vec{w}_l \neq 0$.

We start by stating the Feng-Rao bound for the minimum distance of dual codes.

Definition 4. Let $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ and \mathcal{I} be as above.

An ordered pair $(i, j) \in \mathcal{I} \times \mathcal{I}$ is said to be well-behaving (WB) if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_{j'}) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' \leq i$ and $j' \leq j$ with $(i', j') \neq (i, j)$.

Less restrictive $(i, j) \in \mathcal{I} \times \mathcal{I}$ is said to be weakly well-behaving (WWB) if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ and $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_{j'}) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ hold for all $i' < i$ and $j' < j$.

Even less restrictive $(i, j) \in \mathcal{I} \times \mathcal{I}$ is said to be one-way well-behaving (OWB) if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' < i$.

The usual Feng-Rao bound for the minimum distance of dual codes reads.

Theorem 5. For $\vec{c} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$ write $l = m(\vec{c})$. The Hamming weight of \vec{c} satisfies

$$w_H(\vec{c}) \geq \#\{(i, j) \in \mathcal{I} \times \mathcal{I} \mid \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \text{ and } (i, j) \text{ is OWB}\} \quad (1)$$

$$\geq \#\{(i, j) \in \mathcal{I} \times \mathcal{I} \mid \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \text{ and } (i, j) \text{ is WWB}\} \quad (2)$$

$$\geq \#\{(i, j) \in \mathcal{I} \times \mathcal{I} \mid \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l \text{ and } (i, j) \text{ is WB}\}. \quad (3)$$

From [12, Ex. 2.6] and [15, Sec. 3.1] we have examples where (2) are stronger than (3). Section 4 demonstrates that also (1) can be stronger than (2). This fact was not known before.

Although [15] considered only WB and WWB we shall state our enhancement of the advisory bound using OWB. Doing so we get the strongest possible version which in addition requires the minimal number of calculations.

Definition 6. Let $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ and \mathcal{I} be as above. Consider $\mathcal{I}' = \{i_1, \dots, i_s\} \subseteq \mathcal{I}$ with $i_a \neq i_b$ for $a \neq b$. An ordered pair $(i, j) \in \mathcal{I}' \times \mathcal{I}$ is said to be one-way well-behaving (OWB) with respect to \mathcal{I}' if $\bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j)$ holds for all $i' \in \mathcal{I}'$ with $i' < i$.

We say that \mathcal{I}' has the μ -property with respect to l if for all $i \in \mathcal{I}'$ there exists a $j \in \mathcal{I}$ such that

1. (i, j) is OWB with respect to \mathcal{I}' ,
2. $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$.

The following theorem is an enhancement of the advisory bound [15, Th. 48].

Theorem 7. Let $\vec{c} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$. We have

$$w_H(\vec{c}) \geq \max\{\#\mathcal{I}' \mid \mathcal{I}' \subseteq \mathcal{I}, \mathcal{I}' \text{ has the } \mu\text{-property with respect to } m(\vec{c})\}.$$

Proof. The theorem is a special case of Theorem 14 below. \square

Remark 8. Consider the code $C(s) = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \vec{w}_1 = \dots = \vec{c} \cdot \vec{w}_s = 0\}$. To estimate the minimum distance of $C(s)$ we calculate the minimal value from Theorem 7 when $m(\vec{c})$ runs through all possible numbers in $\{s+1, \dots, n\}$. As an alternative to $C(s)$ we get an improved code construction by using as parity checks only those \vec{w}_l , $l \in \mathcal{I}$ for which Theorem 7 with $m(\vec{c}) = l$ produces values less than δ . The minimum distance of this code, which we denote by $\tilde{C}_{adv}(\delta)$, is at least δ .

We next consider the generalized Hamming weights.

Definition 9. Let $C \subseteq \mathbb{F}_q^n$ be a code of dimension k . For $t = 1, \dots, k$ the t th generalized Hamming weight is

$$d_t(C) = \min\{\# \text{Supp } D \mid D \text{ is a subspace of } C \text{ of dimension } t\}.$$

Clearly, d_1 is nothing but the usual minimum distance. To estimate generalized Hamming weights we first need to extend Definition 6 and Definition 3.

Definition 10. Consider $1 \leq l_1 < \dots < l_t \leq n$ and let $\mathcal{I}' \subseteq \mathcal{I}$. We will say that \mathcal{I}' has the μ -property with respect to $\{l_1, \dots, l_t\}$ if for all $i \in \mathcal{I}'$ there exists a $j \in \mathcal{I}$ such that

- (i, j) is OWB with respect to \mathcal{I}' ,
- $\bar{\rho}_{\mathcal{W}}(\bar{u}_i * \bar{v}_j) \in \{l_1, \dots, l_t\}$.

Definition 11. Let $D \subseteq \mathbb{F}_q^n$ be a subspace. We define

$$m(D) = \{m(\vec{c}) \mid \vec{c} \in D \setminus \{\vec{0}\}\}.$$

The following proposition is easily proved.

Proposition 12. If $D \subseteq \mathbb{F}_q^n$ is a subspace of dimension t then $\#m(D) = t$.

Our enhancement of the advisory bound is based on the following lemma from which we shall also in the next section derive an even better bound.

Lemma 13. Consider a subspace $D \subseteq \mathbb{F}_q^n$. Let $U \subseteq \mathbb{F}_q^n$ be a subspace of dimension δ such that for all non-zero words $\bar{u} \in U$ for some $\bar{v}_j \in \mathcal{V}$ and some $\vec{c} \in D$ it holds that $(\bar{u} * \bar{v}_j) \cdot \vec{c} \neq 0$ then $|\text{Supp } D| \geq \delta$.

Proof. Aiming for a contradiction we assume that the above criteria holds true, but that $|\text{Supp } D| < \delta$. Without loss of generality we write $\text{Supp } D = \{1, \dots, g\}$. Clearly $g \leq \delta - 1$. Consider a matrix whose rows constitute a basis for U . After having performed Gaussian elimination we arrive at a matrix whose last row, say \bar{u}' , starts with $\delta - 1$ zeros. Therefore $\bar{u}' * \vec{c} = \vec{0}$ holds for all $\vec{c} \in D$. On the other hand by assumption for some particular word $\vec{c} \in D$ we have $(\bar{u}' * \bar{v}_j) \cdot \vec{c} \neq 0 \Rightarrow \bar{u}' * \vec{c} \neq \vec{0}$. This is a contradiction. \square

Theorem 14. Consider a subspace $D \subset \mathbb{F}_q^n$. We have

$$\# \text{Supp } D \geq \max\{\#\mathcal{I}' \mid \mathcal{I}' \subseteq \mathcal{I}, \mathcal{I}' \text{ has the } \mu\text{-property with respect to } m(D)\}.$$

Proof. Let $\mathcal{I}' = \{i_1, \dots, i_\delta\}$, $i_a \neq i_b$ for $a \neq b$, be a set which has the μ -property with respect to $m(D)$. Consider $\sum_{r=1}^s \alpha_r \bar{u}_{i_r}$, $1 \leq s \leq \delta$, $\alpha_r \in \mathbb{F}_q$, $\alpha_s \neq 0$. By assumption there exists a $j \in \mathcal{I}$ such that (i_s, j) is OWB with respect to \mathcal{I}' and such that $\bar{\rho}_{\mathcal{W}}(\bar{u}_{i_s} * \bar{v}_j) \in m(D)$. Therefore, $\bar{\rho}_{\mathcal{W}}((\sum_{r=1}^s \alpha_r \bar{u}_{i_r}) * \bar{v}_j) \in m(D)$ and for some $\vec{c} \in D$ it holds that $(\sum_{r=1}^s \alpha_r \bar{u}_{i_r}) * \bar{v}_j \cdot \vec{c} \neq 0$. The theorem now follows from Lemma 13. \square

Remark 15. Let $\{\vec{d}_1, \dots, \vec{d}_{n-k}\} \subseteq \mathbb{F}_q^n$ be a linearly independent set and consider the code $C = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \vec{d}_1 = \dots = \vec{c} \cdot \vec{d}_{n-k} = 0\}$. Without loss of generality we may assume that $\bar{\rho}_{\mathcal{W}}(\vec{d}_1) < \dots < \bar{\rho}_{\mathcal{W}}(\vec{d}_{n-k})$ holds, say these numbers are $l_1 < \dots < l_{n-k}$. It is not hard to prove that $m(C) = \mathcal{I} \setminus \{l_1, \dots, l_{n-k}\}$.

Combining Theorem 14 and Remark 15 we get:

Theorem 16. Let $C = \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \vec{d}_1 = \dots = \vec{c} \cdot \vec{d}_{n-k} = 0\}$, where $\{\vec{d}_1, \dots, \vec{d}_{n-k}\}$ and $\{l_1, \dots, l_{n-k}\}$ are as in Remark 15. For $t = 1, \dots, k$ the t th generalized Hamming weight of C satisfies

$$d_t(C) \geq \min \left\{ \begin{array}{l} \max \{ \#\mathcal{I}' \mid \mathcal{I}' \subseteq \mathcal{I}, \mathcal{I}' \text{ has the } \mu\text{-property with respect to } \{m_1, \dots, m_t\} \} \mid \\ m_1 < \dots < m_t, m_s \in \mathcal{I} \setminus \{l_1, \dots, l_{n-k}\} \text{ for } s = 1, \dots, t \} \end{array} \right\}.$$

In Section 4 we illustrate with a couple of examples that Theorem 16 is operational even though it does appear technical at a first glance.

In a straight forward manner one can enhance Theorem 16 to also deal with relative generalized Hamming weights (See [11, 10]). This bound should be compared with the naive bound, that the relative generalized Hamming weight is always at least as large as the estimate on the generalized Hamming weight from Theorem 16. It should also be compared to the Feng-Rao bound for relative generalized Hamming weights. As we have no examples where the mentioned enhancement of Theorem 16 produces results which are simultaneously better than the above mentioned two alternatives and as at the same time the enhancement of Theorem 16 is rather technical we do not give the details here.

3 Further improvements

In the following we will strengthen the results from the previous section. We start by explaining how to improve upon Theorem 7. Given $\vec{c} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$, consider the corresponding number $m(\vec{c}) = \min\{l \mid \vec{c} \cdot \vec{w}_l \neq 0\}$ and a set $\mathcal{I}' \subseteq \mathcal{I}$ which has the μ -property with respect to $m(\vec{c})$. Theorem 7 relies on the observation that if for $i \in \mathcal{I}'$, $j \in \mathcal{I}$ is the corresponding number such that $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = m(\vec{c})$ and (i, j) is OWB with respect to \mathcal{I}' then

$$\vec{c} \cdot \left(\left(\sum_{\substack{i' \in \mathcal{I}' \\ i' \leq i}} \alpha_{i'} \vec{u}_{i'} \right) * \vec{v}_j \right) \neq 0$$

holds whenever $\alpha_{i'} \in \mathbb{F}_q$, $\alpha_i \neq 0$. Note that the above argument uses no information regarding the status of $\vec{c} \cdot \vec{w}_{m(\vec{c})+1}, \dots, \vec{c} \cdot \vec{w}_n$. Indeed, if the only information we have on \vec{c} is $m(\vec{c})$ then these numbers can take on all possible combinations of values from \mathbb{F}_q .

Remark 17. Let C be as in Remark 15 with

$$\bar{\rho}_{\mathcal{W}}(\vec{d}_1) = l_1 < \dots < \bar{\rho}_{\mathcal{W}}(\vec{d}_{n-k}) = l_{n-k}. \quad (4)$$

Consider a general codeword $\vec{c} \in C \setminus \{\vec{0}\}$. If the only thing we know about $\vec{d}_1, \dots, \vec{d}_{n-k}$ is (4) then we have no information regarding $\vec{c} \cdot \vec{w}_{l_1}, \dots, \vec{c} \cdot \vec{w}_{l_{n-k}}$. If however, as the other extreme, we know that $\vec{d}_1 = \vec{w}_{l_1}, \dots, \vec{d}_{n-k} = \vec{w}_{l_{n-k}}$ then we have $\vec{c} \cdot \vec{w}_{l_1} = \dots = \vec{c} \cdot \vec{w}_{l_{n-k}} = 0$.

Write $l = m(\vec{c})$ and consider the indexes $l+1, \dots, l+v \leq n$. Here, v is some positive integer. For some of the above indexes x we may *a priori* know that $\vec{c} \cdot \vec{w}_x = 0$ (Remark 17). Let l'_1, \dots, l'_s be the remaining indexes from $\{l+1, \dots, l+v\}$. The idea in our improvement to Theorem 7 is to consider separately the following $s+1$ cases:

$$\text{Case 0: } \vec{c} \cdot \vec{w}_{l'_1} = \dots = \vec{c} \cdot \vec{w}_{l'_s} = 0.$$

$$\text{Case 1: } \vec{c} \cdot \vec{w}_{l'_1} \neq 0.$$

$$\text{Case 2: } \vec{c} \cdot \vec{w}_{l'_1} = 0, \vec{c} \cdot \vec{w}_{l'_2} \neq 0.$$

$$\vdots$$

$$\text{Case } s: \vec{c} \cdot \vec{w}_{l'_1} = \dots = \vec{c} \cdot \vec{w}_{l'_{s-1}} = 0, \vec{c} \cdot \vec{w}_{l'_s} \neq 0.$$

In each case z we establish a set $\mathcal{I}'_z \subseteq \mathcal{I}$ such that for every non-zero linear combination $\sum_{i \in \mathcal{I}'_z} \alpha_i \vec{u}_i$, $\alpha_i \in \mathbb{F}_q$, a $\vec{v}_j \in \mathcal{V}$ exists with

$$\vec{c} \cdot \left(\left(\sum_{i \in \mathcal{I}'_z} \alpha_i \vec{u}_i \right) * \vec{v}_j \right) \neq 0.$$

From Lemma 13 it then follows that $w_H(\vec{c}) \geq \min\{\#\mathcal{I}'_0, \dots, \#\mathcal{I}'_s\}$. The following definition is what we need to deal with the above set-up. We should stress that although Definition 18 may appear long and technical, it is often quite manageable. This will be demonstrated in Section 4.

Definition 18. Consider the numbers $1 \leq l, l+1, \dots, l+g \leq n$. A set $\mathcal{I}' \subseteq \mathcal{I}$ is said to have the μ -property with respect to l with exception $\{l+1, \dots, l+g\}$ if for all $i \in \mathcal{I}'$ a $j \in \mathcal{I}$ exists such that

$$(1a) \quad \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l, \text{ and}$$

$$(1b) \quad \text{for all } i' \in \mathcal{I}' \text{ with } i' < i \text{ either } \bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) < l \text{ or } \bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) \in \{l+1, \dots, l+g\} \text{ holds.}$$

Assume next that $l+g+1 \leq n$. The set \mathcal{I}' is said to have the relaxed μ -property with respect to $(l, l+g+1)$ with exception $\{l+1, \dots, l+g\}$ if for all $i \in \mathcal{I}'$ a $j \in \mathcal{I}$ exists such that either conditions (1a) and (1b) above hold or

$$(2a) \quad \bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l+g+1, \text{ and}$$

$$(2b) \quad (i, j) \text{ is OWB with respect to } \mathcal{I}', \text{ and}$$

$$(2c) \quad \text{no } i' \in \mathcal{I}' \text{ with } i' < i \text{ satisfies } \bar{\rho}_{\mathcal{W}}(\vec{u}_{i'} * \vec{v}_j) = l.$$

From the discussion above we arrive at the following improvement to Theorem 7.

Theorem 19. Consider a non-zero codeword \vec{c} and let $l = m(\vec{c})$. Choose a non-negative integer v such that $l+v \leq n$. Assume that for some indexes $x \in \{l+1, \dots, l+v\}$ we know *a priori* that $\vec{c} \cdot \vec{w}_x = 0$. Let $l'_1 < \dots < l'_s$ be the remaining indexes from $\{l+1, \dots, l+v\}$. Consider the sets $\mathcal{I}'_0, \mathcal{I}'_1, \dots, \mathcal{I}'_s$ such that:

- \mathcal{I}'_0 has the μ -property with respect to l with exception $\{l+1, \dots, l+v\}$.
- For $i = 1, \dots, s$, \mathcal{I}'_i has the relaxed μ -property with respect to (l, l'_i) with exception $\{l+1, \dots, l'_i-1\}$.

We have

$$w_H(\vec{c}) \geq \min\{\#\mathcal{I}'_0, \#\mathcal{I}'_1, \dots, \#\mathcal{I}'_s\}. \quad (5)$$

To establish a lower bound on the minimum distance of a code C we repeat the above process for each $l \in m(C)$. For each such l we choose a corresponding v , we determine sets \mathcal{I}'_i as above and we calculate the right side of (5). The smallest value found constitutes a lower bound on the minimum distance.

Remark 20. The results in Remark 8 also hold if we replace Theorem 7 with Theorem 19. We shall denote the resulting improved codes by $\tilde{C}_{\text{fim}}(\delta)$ (here, *fim* stands for further improved).

Remark 21. Assume \mathcal{I}' has the μ -property with respect to l . One possible choice of sets $\mathcal{I}'_0, \mathcal{I}'_1, \dots, \mathcal{I}'_s \subseteq \mathcal{I}$ in Theorem 19 would be to choose all of them to be equal to \mathcal{I}' . It follows that Theorem 19 is indeed at least as strong as Theorem 7. The above observation relates to the fact that Theorem 19 reduces to Theorem 7 when v is chosen to be always equal to 0.

As shall be demonstrated later in the paper, Theorem 19 can sometimes be much better than Theorem 7. For Theorem 19 to be operational we need a clever method to choose for each $l \in m(C)$ the corresponding number v . As shall be clear from the examples in Section 4 for affine variety codes there is a very natural way to do this. Another remark is that when the task is to estimate the minimum distance of a fixed code, then we can set v equal to 0 for most values of l , reserving non-zero values to those l for which Theorem 7 produces the smallest numbers. These are the numbers that need to be improved.

In a similar way as Theorem 7 was enhanced to deal with generalized Hamming weights and relative generalized Hamming weights we can enhance Theorem 19. The notation in Definition 18 being already involved we only illustrate how to deal with the second generalized Hamming weight. From that description it should be clear how to deal with higher weights.

Proposition 22. Let the notation be as in Theorem 19. Consider a subspace $D \subseteq C$ of dimension 2, say $m(D) = \{a, b\}$. Let v_a be the v corresponding to $l = a$. Let $a'_1 < \dots < a'_{s_a}$ be the numbers $l'_1 < \dots < l'_s$ corresponding to $l = a$. Analogously for the case b . Referring to Definition 18, for $\alpha = 1, \dots, s_a$ and $\beta = 1, \dots, s_b$ we define subsets of \mathcal{I} as follows:

- $\mathcal{I}''_{0,0}$ is a set such that for all $i \in \mathcal{I}''_{0,0}$ for an $l \in \{a, b\}$ a j exists such that (1a) and (1b) hold with $g = v_a$ if $l = a$, and $g = v_b$ if $l = b$.
- $\mathcal{I}''_{\alpha,0}$ is a set such that for all $i \in \mathcal{I}''_{\alpha,0}$ a j exists such that one of the following two conditions holds:
 - Either (1a), (1b) or (2a), (2b), (2c) hold with $l = a$ and $g+1 = a'_\alpha$.
 - (1a) and (1b) hold with $l = b$ and $g = v_b$.
- $\mathcal{I}''_{0,\beta}$ is defined similarly to $\mathcal{I}''_{\alpha,0}$.

- $\mathcal{I}''_{\alpha,\beta}$ is a set such that for all $i \in \mathcal{I}''_{\alpha,\beta}$ an $l \in \{a, b\}$ and a $j \in \mathcal{I}$ exist such that either (1a), (1b) or (2a), (2b), (2c) hold. Here, $g + 1 = a'_\alpha$ if $l = a$, and $g + 1 = b'_\beta$ if $l = b$.

The support of D is of size at least equal to the smallest cardinality of the above sets. To establish a lower bound on the second generalized Hamming weight of a code C we repeat the above process for each $(a, b) \in m(C) \times m(C)$ with $a < b$. The smallest value found constitutes a lower bound on the second generalized Hamming weight.

Applying in larger generality the method described in the above proposition we derive lower bounds on any generalized Hamming weights of C . It is clear that this method can be of much higher complexity than the method described in Theorem 16. To lower the complexity we choose (referring to the case of the second weight) most v_a and v_b equal to zero, reserving non-zero values to those (a, b) for which Theorem 16 produces low values. As shall be demonstrated in the following section, Proposition 22 and its generalization to higher weights can sometimes produce much better results than Theorem 16. Similar results on the relative generalized Hamming weights as those mentioned at the end of Section 2 hold for the method described above.

4 Examples

In this section we apply the advisory bound and the improved bound from Section 3 to affine variety codes coming from two particular curves. The first curve corresponds to [15, Sec. 3.1]. It is a plane curve over \mathbb{F}_8 . The second curve is the natural counterpart for the field \mathbb{F}_{27} . We shall need a couple of results from Gröbner basis theory.

4.1 Some results from Gröbner basis theory

Let \prec be a monomial ordering on the set of monomials in X_1, \dots, X_m . Given an ideal $J \subseteq k[X_1, \dots, X_m]$, where k is a field, the footprint $\Delta_\prec(J)$ is the set of monomials that can not be found as leading monomial of any polynomial in J . A Gröbner basis, by definition, is a generating set for J from which the footprint can be easily read of. More formally, $\{L_1(X_1, \dots, X_m), \dots, L_s(X_1, \dots, X_m)\} \subseteq J$ is a Gröbner basis for J with respect to \prec if for any $F(X_1, \dots, X_m) \in J$ for some $i \in \{1, \dots, s\}$ it holds that $\text{lm}(L_i) | \text{lm}(F)$. Recall that $\{M + J \mid M \in \Delta_\prec(J)\}$ is a basis for the quotient ring $k[X_1, \dots, X_m]/J$ as a vector space over k . In the following we shall assume that $k = \mathbb{F}_q$ and that J contains all the equations $X_1^q - X_1, \dots, X_m^q - X_m$, in which case we write $J = I_q$. Obviously, the variety of I_q is finite. Let the variety be $\{P_1, \dots, P_n\}$ and consider the evaluation map $\text{ev} : \mathbb{F}_q[X_1, \dots, X_m]/I_q \rightarrow \mathbb{F}_q^n$ given by $\text{ev}(F + I_q) = (F(P_1), \dots, F(P_n))$. It is well-known that this map is a vector space isomorphism implying that $n = \#\Delta_\prec(I_q)$ holds. If we embark the vector space \mathbb{F}_q^n with a second binary operation, namely the component wise product from Definition 2 then it becomes an \mathbb{F}_q -algebra. It is not difficult to see that the map ev in this way becomes an isomorphism between \mathbb{F}_q -algebras. Hence, if we enumerate the elements of $\Delta_\prec(I_q) = \{M_1, \dots, M_n\}$ according to \prec and define $\mathcal{U} = \mathcal{V} = \mathcal{W} = \{\vec{b}_1 =$

Y^7	XY^7	X^2Y^7	X^3Y^7	14	17	20	23	21	26	30	32
Y^6	XY^6	X^2Y^6	X^3Y^6	12	15	18	21	17	23	28	31
Y^5	XY^5	X^2Y^5	X^3Y^5	10	13	16	19	13	19	25	29
Y^4	XY^4	X^2Y^4	X^3Y^4	8	11	14	17	9	15	22	27
Y^3	XY^3	X^2Y^3	X^3Y^3	6	9	12	15	6	11	18	24
Y^2	XY^2	X^2Y^2	X^3Y^2	4	7	10	13	4	8	14	20
Y	XY	X^2Y	X^3Y	2	5	8	11	2	5	10	16
1	X	X^2	X^3	0	3	6	9	1	3	7	12

Monomials in Δ_{\prec_w}

Corresponding weights

Indexing of \mathcal{W}

Figure 1:

$\text{ev}(M_1 + I_q), \dots, \vec{b}_n = \text{ev}(M_n + I_q)\}$ then we can translate information on the algebraic structure of $\mathbb{F}_q[X_1, \dots, X_m]/I_q$ into information regarding the well-behaving properties as introduced in Definition 4, 6, 10, 18 and Proposition 22. We shall illustrate how to do this in the following.

4.2 Codes from a curve over \mathbb{F}_8

In [15, Sec. 3.1] Salazar et. al. considered curves of the form $F_8(X, Y) = G_8(X) - H_8(Y) \in \mathbb{F}_8[X, Y]$ where $G_8(X)$ is a polynomial of degree 4 and $H_8(Y)$ is a polynomial of degree 6 both having the property that when evaluated in \mathbb{F}_8 they return values in \mathbb{F}_2 . It is of no implication to the estimation of code parameters if we restrict to $G_8(X)$ being the trace polynomial $X^4 + X^2 + X$ and if we choose $H_8(Y) = Y^6 + Y^5 + Y^3$. Consider the trace-polynomial corresponding to a general field extension. It is well-known that the preimages of all the elements in the ground field are of the same size. From this we conclude that the particular polynomial $F_8(X, Y) = G_8(X) - H_8(Y)$ under consideration has exactly $2^5 = 32$ zeros.

Let $I_8 = \langle F_8(X, Y), X^8 - X, Y^8 - Y \rangle \subseteq \mathbb{F}_8[X, Y]$. From the above discussion we know that the corresponding variety is of size 32. If we consider a monomial ordering such that $\text{lm}(F_8) = X^4$ then there exist exactly 32 monomials which are not divisible by any of the monomials $\text{lm}(F_8) = X^4, \text{lm}(Y^8 - Y) = Y^8$. Hence, $\{F_8(X, Y), Y^8 - Y\}$ is a Gröbner basis for I_8 and $\Delta_{\prec}(I_8) = \{X^\alpha Y^\beta \mid 0 \leq \alpha < 4, 0 \leq \beta < 8\}$ holds. In the following we consider a particular weighted degree lexicographic ordering for which $\text{lm}(F_8) = X^4$ holds. Let $w(X) = 3$, $w(Y) = 2$, and in general $w(X^\alpha Y^\beta) = 3\alpha + 2\beta$. We define \prec_w to be the monomial ordering given by $X^{\alpha_1} Y^{\beta_1} \prec_w X^{\alpha_2} Y^{\beta_2}$ if either $w(X^{\alpha_1} Y^{\beta_1}) < w(X^{\alpha_2} Y^{\beta_2})$ or if alternatively $w(X^{\alpha_1} Y^{\beta_1}) = w(X^{\alpha_2} Y^{\beta_2})$ and $\alpha_1 < \alpha_2$ hold.

Let $\Delta_{\prec_w}(I_8) = \{M_1, \dots, M_{32}\}$, the monomials being enumerated with respect to \prec_w . For the code construction we consider the basis $\mathcal{W} = \{\vec{w}_1 = \text{ev}(M_1 + I_8), \dots, \vec{w}_{32} = \text{ev}(M_{32} + I_8)\}$. The situation is described in Figure 1. We then set $\vec{u}_i = \vec{v}_i = \vec{w}_i$ for $i = 1, \dots, 32$ defining the bases \mathcal{U} and \mathcal{V} .

By definition, $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = l$ if and only if

$$\text{lm}(M_i M_j \text{ rem } \{F_8(X, Y), X^8 - X, Y^8 - Y\}) = M_l.$$

Further, (i, j) is WB if and only if

$$\text{lm}(M_{i'} M_{j'} \text{ rem } \{F_8(X, Y), X^8 - X, Y^8 - Y\}) \prec_w M_l \quad (6)$$

holds for all $i' \leq i$ and $j' \leq j$ with $(i', j') \neq (i, j)$. There are two particular easy cases to analyze:

- **Rule (I):** If $M_i M_j = M_l$ then by the property of a monomial ordering (6) holds.
- **Rule (II):** If $w(M_i) + w(M_j) = w(M_l)$ and $w(M_{i'}) < w(M_i)$ for all $i' < i$ and if $w(M_{j'}) < w(M_j)$ for all $j' < j$, then (6) holds.

In a straightforward manner one derives similar rules regarding WWB and OWB.

Consider $l = 17$. Using Rule (I) we see that every

$$(i, j) \in \{(1, 17), (2, 13), (4, 9), (6, 6), (9, 4), (13, 2), (17, 1)\}$$

is WB with $\bar{\rho}_{\mathcal{W}}(\vec{u}_i * \vec{v}_j) = 17$.

We have $\bar{\rho}_{\mathcal{W}}(\vec{u}_3 * \vec{v}_{12}) = 17$ as

$$\begin{aligned} & \text{lm}(M_3 M_{12} \text{ rem } \{F_8(X, Y), X^8 - X, Y^8 - Y\}) \\ &= \text{lm}(X^4 \text{ rem } \{F_8(X, Y), X^8 - X, Y^8 - Y\}) \\ &= \text{lm}(Y^6 + Y^5 + X^2 + Y^3 + X) = Y^6 = M_{17}. \end{aligned}$$

But $M_3 M_{11} = M_{18}$ implying that $\bar{\rho}_{\mathcal{W}}(\vec{u}_3 * \vec{v}_{11}) = 18$. Therefore $(3, 12)$ is not WWB. However $w(M_{i'}) < w(M_3)$ for all $i' < 3$ and by a result similar to Rule (II), $(3, 12)$ therefore is OWB.

We next claim that $\mathcal{I}' = \{1, 2, 4, 6, 9, 13, 17, 3, 12\}$ has the μ -property with respect to 17. To this end, the only thing missing to be checked is the case $i = 12$. Clearly, $\bar{\rho}_{\mathcal{W}}(\vec{u}_{12} * \vec{v}_3) = 17$. Note that $w(M_{12}) = 9$ does not belong to $\{w(M_i) \mid i \in \mathcal{I}' \setminus \{12\}\}$ and by an argument similar to Rule (II) we conclude that $(12, 3)$ is OWB with respect to \mathcal{I}' .

We next apply Theorem 19 with $l = 17$ and $v = 1$. Note that $w(M_{17}) = w(M_{18}) < w(M_{19})$ which is what makes the choice $v = 1$ natural. Using similar arguments as above we see that

$$\mathcal{I}'_0 = \{1, 2, 4, 6, 9, 13, 17, 3, 12\} \cup \{7\}$$

has the μ -property with respect to 17 with exception $\{18\}$ and that

$$\mathcal{I}'_1 = \{1, 2, 4, 6, 9, 13, 17\} \cup \{3, 5, 8, 11\}$$

has the relaxed μ -property with respect to $(17, 18)$ with exception $\{7\}$. Clearly, \mathcal{I}'_0 is the smallest of these two sets.

In conclusion, if $m(\vec{c}) = 17$ we get the following estimates:

- The Feng-Rao bound in the version with WB or WWB gives $w_H(\vec{c}) \geq 7$.

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	Advisory bound	Section 3
d_1	7	7	8	9	10
d_2	8	8	10	12	13

Table 1: Estimates on first and second generalized Hamming weight of the code $C(16)$ over \mathbb{F}_8 .

- The same bound in the version with OWB produces $w_H(\vec{c}) \geq 8$.
- From the advisory bound we get $w_H(\vec{c}) \geq 9$.
- Finally, our new bound produces $w_H(\vec{c}) \geq 10$.

Applying exactly the same techniques as above we get the following estimates of $w_H(\vec{c})$ when $m(\vec{c}) = 21$:

- The Feng-Rao bound with WB or WWB gives $w_H(\vec{c}) \geq 8$.
- The same bound in the version with OWB produces $w_H(\vec{c}) \geq 10$.
- From the advisory bound we get $w_H(\vec{c}) \geq 12$ (This is done by choosing $\mathcal{I}' = \{1, 2, 4, 6, 9, 13, 17, 21\} \cup \{3, 5, 12, 16\}$).
- Finally, our new bound produces $w_H(\vec{c}) \geq 13$ (This is done by choosing $v = 1$, $\mathcal{I}'_0 = \{1, 2, 4, 6, 9, 13, 17, 21\} \cup \{3, 7, 12, 5, 10, 16\}$ and $\mathcal{I}'_1 = \{1, 2, 4, 6, 9, 13, 17, 21\} \cup \{3, 5, 8, 11, 15\}$).

For the remaining choices of $l \in \mathcal{I}$ neither the advisory bound nor the improved bound from the present paper produces better results than the Feng-Rao bound with WWB. As explained in [15] for $m(\vec{c}) = 28$ and $m(\vec{c}) = 30$, respectively, the Feng-Rao bound with WWB improves upon the same bound with WB by lifting the estimates from 21 to 22 and from 24 to 26, respectively.

We first consider the codes $C(s)$ (See Remark 8 for the definition). In Figure 2 we illustrate the parameters $k, d_1(C(s)), \dots, d_5(C(s))$. As is seen, for all of the five choices of bounds: the Feng-Rao bound with WB, WWB, OWB, the advisory bound, and the bound from Section 3, there exist numbers i and s such that the best estimate on $d_i(C(s))$ is obtained by this particular bound (and consequently also by the sharper bounds as well). Regarding the 6th generalized Hamming weight, only for one s we can improve upon what is derived from the Feng-Rao bound with WB. Namely, for $C(4)$ where the Feng-Rao bound with WB or WWB produces the estimate 8 whereas all other bounds give 9. In Table 1 we illustrate that the various bounds sometimes improve very much on each other by showing estimates for the first two weights of the code $C(16)$. For this particular code for higher weights all estimates are the same.

We next consider the improved codes $\tilde{C}_{adv}(\delta)$ and $\tilde{C}_{fim}(\delta)$ (See Remark 8 and Remark 20 for the definitions). For two designed distances $\delta = 10, 13$, the code $\tilde{C}_{fim}(\delta)$ is of higher dimension than $\tilde{C}_{adv}(\delta)$. In Table 2 we list estimates from the advisory bound on the generalized Hamming weights of the first code and estimates from the bound of Section 3 on the generalized Hamming weights of the latter code, respectively. We see that for higher generalized Hamming weights there is a price to be paid for the increase in dimension.

dimension					d_1					d_2				
Υ^7	12	7	3	1	Υ^7	13^5	16^1	26^2	32^1	Υ^7	15^1	24^2	31^1	—
Υ^6	16	10	5	2	Υ^6	10^5	14^1	22^2	28^1	Υ^6	13^5	16^1	26^2	32^1
Υ^5	20	14	8	4	Υ^5	6^1	12^4	16^1	24^1	Υ^5	9^4	14^1	22^2	28^1
Υ^4	24	18	11	6	Υ^4	4^1	8^3	14^1	20^1	Υ^4	6^1	12^4	16^1	24^1
Υ^3	27	22	15	9	Υ^3	3^1	4^1	12^4	16^1	Υ^3	4^1	8^3	14^1	20^1
Υ^2	29	25	19	13	Υ^2	3^1	4^1	8^3	12^4	Υ^2	4^1	6^1	11^4	15^1
Υ	31	28	23	17	Υ	2^1	3^1	4^1	8^3	Υ	3^1	4^1	7^1	12^4
1	32	30	26	21	1	1^1	2^1	3^1	4^1	1	2^1	3^1	4^1	8^3
	1	X	X^2	X^3		1	X	X^2	X^3		1	X	X^2	X^3

d_3					d_4					d_5				
Υ^7	16^1	26^2	32^1	—	Υ^7	21^1	28^1	—	—	Υ^7	22^1	30^1	—	—
Υ^6	14^1	22^2	28^1	—	Υ^6	15^1	24^2	31^1	—	Υ^6	16^1	26^1	32^1	—
Υ^5	12^4	15^1	24^2	31^1	Υ^5	13^1	16^1	26^2	32^1	Υ^5	14^1	21^1	28^1	—
Υ^4	8^3	13^1	20^1	27^1	Υ^4	10^3	14^1	22^2	28^1	Υ^4	12^3	15^1	24^1	31^1
Υ^3	6^1	10^3	15^1	23^1	Υ^3	8^3	12^3	16^1	24^1	Υ^3	9^3	13^1	20^1	27^1
Υ^2	5^1	8^3	12^1	16^1	Υ^2	6^1	10^3	14^1	20^1	Υ^2	8^3	11^1	20^1	22^1
Υ	4^1	6^1	8^1	14^1	Υ	5^1	7^1	11^1	15^1	Υ	6^1	8^1	12^1	16^1
1	3^1	4^1	7^1	10^3	1	4^1	6^1	8^1	12^3	1	5^1	7^1	10^1	14^1
	1	X	X^2	X^3		1	X	X^2	X^3		1	X	X^2	X^3

Figure 2: The figure lists the dimensions of codes $C(s)$ over \mathbb{F}_8 and corresponding estimates on d_1, \dots, d_5 . Information about $C(s)$ is placed at the position of \bar{w}_{s+1} . An entry z^1 means that the value z was obtained from the Feng-Rao bound with WB, z^2 indicate that the same bound with WWB was used, and finally z^3 the same bound with OWB. With z^4 we indicate that the value z was obtained from the advisory bound and by z^5 that the method from Section 3 was used. The symbol - inside the table indicates that the corresponding parameter does not exist.

	k	d_2	d_3	d_4	d_5	d_6
$\tilde{C}_{adv}(10)$	16	12	14	15	16	20
$\tilde{C}_{fim}(10)$	17	12	13	14	15	16
$\tilde{C}_{adv}(13)$	11	16	20	22	24	26
$\tilde{C}_{fim}(13)$	12	15	16	21	22	24

Table 2: Parameters of improved codes over \mathbb{F}_8 . By definition, the codes $\tilde{C}_{adv}(10)$ and $\tilde{C}_{fim}(10)$ are of designed minimum distance 10. Similarly, $\tilde{C}_{adv}(13)$ and $\tilde{C}_{fim}(13)$, are of designed minimum distance 13. By k we denote the dimension. The values of d_2, \dots, d_6 for $\tilde{C}_{adv}(10)$ and $\tilde{C}_{adv}(13)$ are estimated using the advisory bound. For $\tilde{C}_{fim}(10)$ and $\tilde{C}_{fim}(13)$ the method from Section 3 is used.

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	Advisory bound	Section 3
$d_1(C(75))$	15	15	21	29	33
$d_2(C(75))$	16	16	24	34	38
$d_1(C(76))$	15	15	21	33	36
$d_2(C(76))$	16	16	24	38	39
$d_1(C(83))$	16	16	24	34	38
$d_2(C(83))$	17	17	27	39	41

Table 3: Estimates of minimum distance and second generalized Hamming weight for a selection of codes over \mathbb{F}_{27} .

4.3 Codes from a curve over \mathbb{F}_{27}

Similarly to the curve $F_8(X, Y) \in \mathbb{F}_8[X, Y]$ from the previous section we now consider the curve $F_{27}(X, Y) = G_{27}(X) - H_{27}(Y) \in \mathbb{F}_{27}[X, Y]$. Here, $G_{27}(X)$ is the trace-polynomial $X^9 + X^3 + X$ and $H_{27}(Y) = Y^{12} + Y^{10} + Y^4$ satisfies that when evaluated in elements from \mathbb{F}_{27} it returns values from \mathbb{F}_3 . The arguments of the previous subsection translate immediately. Only difference is that now instead of having many pairs of monomials in the footprint being of the same weight we now have many triples of monomials in the footprint being of the same weight. The implication is that when applying Theorem 19 we will often need $v = 2$ rather than $v = 1$. The codes being of length $n = 3^5 = 243$ we cannot give many details, but restrict to consider the minimum distance and the second generalized Hamming weight of the codes $C(s)$. See Figure 3. Again, all five bounds come into action. To illustrate how much the advisory bound and the bound of Section 3 improve upon the various versions of the Feng-Rao bound we treat in detail the codes $C(75)$, $C(76)$, $C(83)$ in Table 3. These codes are of dimension 168, 167 and 160.

5 Concluding remarks

In this paper we treated two improvements to the Feng-Rao bound for dual codes: the advisory bound and a new bound which is an improvement to it. The latter bound is closely related to a new bound for primary codes which we treat in a separate paper. Part of this research was done while the second listed author was visiting East China Normal University. We are grateful to Professor Hao Chen for his hospitality. The authors also gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography.

	dimension										d_1								
γ^{26}	54	43	33	24	17	11	6	3	1	γ^{26}	73 ⁴	77 ⁴	81 ¹	138 ³	150 ³	162 ¹	219 ²	231 ²	243 ¹
γ^{25}	63	51	40	30	22	15	9	5	2	γ^{25}	70 ⁴	74 ⁴	78 ¹	132 ³	144 ³	156 ¹	210 ²	222 ²	234 ¹
γ^{24}	72	60	48	37	28	20	13	8	4	γ^{24}	67 ⁴	71 ⁴	75 ⁴	81 ¹	138 ³	150 ³	162 ¹	213 ²	225
γ^{23}	81	69	57	45	35	26	18	12	7	γ^{23}	64 ⁴	68 ⁴	72 ⁴	77 ⁴	81 ¹	138 ³	150 ³	162 ¹	216
γ^{22}	90	78	66	53	42	32	23	16	10	γ^{22}	61 ⁴	65 ⁴	69 ⁴	74 ⁴	78 ¹	132 ³	144 ³	156 ³	207 ²
γ^{21}	99	87	75	62	50	39	29	21	14	γ^{21}	58 ⁴	62 ⁴	66 ⁴	71 ⁴	75 ⁴	81 ¹	138 ³	150 ³	162 ¹
γ^{20}	108	96	84	71	59	47	36	27	19	γ^{20}	55 ⁴	59 ⁴	63 ⁴	68 ⁴	72 ⁴	77 ⁴	81 ¹	138 ³	150 ³
γ^{19}	117	105	93	80	68	56	44	34	25	γ^{19}	52 ⁴	56 ⁴	60 ⁴	65 ⁴	69 ⁴	73 ⁴	77 ⁴	81 ¹	138 ³
γ^{18}	126	114	102	89	77	65	52	41	31	γ^{18}	49 ⁴	53 ⁴	57 ⁴	62 ⁴	66 ⁴	70 ⁴	74 ⁴	78 ¹	132 ³
γ^{17}	135	123	111	98	86	74	61	49	38	γ^{17}	46 ⁴	50 ⁴	54 ⁴	59 ⁴	63 ⁴	67 ⁴	71 ⁴	75 ⁴	81 ¹
γ^{16}	144	132	120	107	95	83	70	58	46	γ^{16}	43 ⁴	47 ⁴	51 ⁴	56 ⁴	60 ⁴	64 ⁴	68 ⁴	72 ⁴	77 ⁴
γ^{15}	153	141	129	116	104	92	79	67	55	γ^{15}	40 ⁵	44 ⁴	48 ⁴	53 ⁴	57 ⁴	61 ⁴	65 ⁴	69 ⁴	73 ⁴
γ^{14}	162	150	138	125	113	101	88	76	64	γ^{14}	37 ⁵	41 ⁵	45 ⁴	50 ⁴	54 ⁴	58 ⁴	62 ⁴	66 ⁴	70 ⁴
γ^{13}	171	159	147	134	122	110	97	85	73	γ^{13}	30 ⁵	38 ⁵	42 ⁴	47 ⁴	51 ⁴	55 ⁴	59 ⁴	63 ⁴	67 ⁴
γ^{12}	180	168	156	143	131	119	106	94	82	γ^{12}	21 ⁵	33 ⁵	39 ⁴	44 ⁴	48 ⁴	52 ⁴	56 ⁴	60 ⁴	64 ⁴
γ^{11}	189	177	165	152	140	128	115	103	91	γ^{11}	12 ¹	24 ⁴	36 ⁵	41 ⁵	45 ⁴	49 ⁴	53 ⁴	57 ⁴	61 ⁴
γ^{10}	198	186	174	161	149	137	124	112	100	γ^{10}	9 ¹	18 ⁴	27 ⁵	38 ⁵	42 ⁴	46 ⁴	50 ⁴	54 ⁴	58 ⁴
γ^9	206	195	183	170	158	146	133	121	109	γ^9	8 ¹	9 ¹	18 ⁴	33 ⁵	39 ⁴	43 ⁴	47 ⁴	51 ⁴	55 ⁴
γ^8	213	203	192	179	167	155	142	130	118	γ^8	7 ¹	8 ¹	9 ¹	24 ⁴	36 ⁵	40 ⁵	44 ⁴	48 ⁴	52 ⁴
γ^7	219	210	200	188	176	164	151	139	127	γ^7	7 ¹	8 ¹	9 ¹	18 ⁴	27 ⁵	36 ⁵	41 ⁵	45 ⁴	49 ⁴
γ^6	225	217	208	197	185	173	160	148	136	γ^6	6 ¹	7 ¹	8 ¹	9 ¹	18 ⁴	27 ⁵	38 ⁵	42 ⁴	46 ⁴
γ^5	230	223	215	205	194	182	169	157	145	γ^5	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	18 ⁴	33 ⁵	39 ⁵	43 ⁴
γ^4	234	228	221	212	202	191	178	166	154	γ^4	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	24 ⁴	36 ⁵	40 ⁵
γ^3	237	232	226	218	209	199	187	175	163	γ^3	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	18 ⁴	27 ⁵	36 ⁵
γ^2	240	236	231	224	216	207	196	184	172	γ^2	3 ¹	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	18 ⁴	27 ⁵
γ	242	239	235	229	222	214	204	193	181	γ	2 ¹	3 ¹	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	18 ⁴
1	243	241	238	233	227	220	211	201	190	1	1 ¹	2 ¹	3 ¹	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹
	1	X	X ²	X ³	X ⁴	X ⁵	X ⁶	X ⁷	X ⁸		1	X	X ²	X ³	X ⁴	X ⁵	X ⁶	X ⁷	X ⁸

	d_2								
γ^{26}	76	80 ¹	135 ³	149 ³	161 ¹	216 ²	230 ²	242 ¹	—
γ^{25}	73 ⁴	77 ⁴	81 ¹	138 ³	150 ³	162 ¹	219 ²	231 ²	243 ¹
γ^{24}	70 ⁴	74 ⁴	78 ¹	132 ³	144 ³	156 ¹	210 ²	222 ²	234 ¹
γ^{23}	67 ⁴	71 ⁴	75 ⁴	80 ¹	135 ³	149 ³	161 ¹	213 ²	225 ²
γ^{22}	64 ⁴	68 ⁴	72 ⁴	77 ⁴	81 ¹	138 ³	150 ³	162 ¹	216 ²
γ^{21}	61 ⁴	65 ⁴	69 ⁴	74 ⁴	78 ¹	132 ³	144 ³	156 ¹	207 ²
γ^{20}	58 ⁴	62 ⁴	66 ⁴	71 ⁴	75 ⁴	80 ¹	135 ³	149 ³	161 ¹
γ^{19}	55 ⁴	59 ⁴	63 ⁴	68 ⁴	72 ⁴	76 ⁴	80 ¹	135 ³	149 ³
γ^{18}	52 ⁴	56 ⁴	60 ⁴	65 ⁴	69 ⁴	73 ⁴	77 ⁴	81 ¹	138 ³
γ^{17}	49 ⁴	53 ⁴	57 ⁴	62 ⁴	66 ⁴	70 ⁴	74 ⁴	78 ¹	132 ³
γ^{16}	46 ⁴	50 ⁴	54 ⁴	59 ⁴	63 ⁴	67 ⁴	71 ⁴	75 ⁴	80 ¹
γ^{15}	43 ⁴	47 ⁴	51 ⁴	56 ⁴	60 ⁴	64 ⁴	68 ⁴	72 ⁴	76 ⁴
γ^{14}	40 ⁵	44	48 ⁴	53 ⁴	57 ⁴	61 ⁴	65 ⁴	69 ⁴	73 ⁴
γ^{13}	37 ⁵	41 ⁵	45 ⁴	50 ⁴	54 ⁴	58 ⁴	62 ⁴	66 ⁴	70 ⁴
γ^{12}	30 ⁵	38 ⁵	42 ⁴	47 ⁴	51 ⁴	55 ⁴	59 ⁴	63 ⁴	67 ⁴
γ^{11}	21 ⁵	33 ⁵	39 ⁴	44 ⁴	48 ⁴	52 ⁴	56 ⁴	60 ⁴	64 ⁴
γ^{10}	12 ¹	24 ⁴	36 ⁵	41 ⁵	45 ⁴	49 ⁴	53 ⁴	57 ⁴	61 ⁴
γ^9	9 ¹	17 ⁴	27 ⁵	38 ⁵	42 ⁴	46 ⁴	50 ⁴	54 ⁴	58 ⁴
γ^8	8 ¹	9 ¹	18 ⁴	33 ⁵	39 ⁵	43 ⁴	47 ⁴	51 ⁴	55 ⁴
γ^7	8 ¹	9 ¹	12 ¹	24 ⁴	35 ⁵	40 ⁵	44 ⁴	48 ⁴	52 ⁴
γ^6	7 ¹	8 ¹	9 ¹	17 ⁴	26 ⁴	36 ⁵	41 ⁵	45 ⁴	49 ⁴
γ^5	6 ¹	7 ¹	8 ¹	9 ¹	17 ⁴	27 ⁵	38 ⁵	42 ⁴	46 ⁴
γ^4	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	18 ⁴	33 ⁵	39 ⁵	43 ⁴
γ^3	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	12 ¹	24 ⁴	35 ⁵	40 ⁵
γ^2	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	17 ⁴	26 ⁴	36 ⁵
γ	3 ¹	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	17 ⁴	27 ⁵
1	2 ¹	3 ¹	4 ¹	5 ¹	6 ¹	7 ¹	8 ¹	9 ¹	18 ⁴
	1	X	X ²	X ³	X ⁴	X ⁵	X ⁶	X ⁷	X ⁸

Figure 3: Dimensions, minimum distance and second generalized Hamming weight of codes $C(s)$ over \mathbb{F}_{27} . Notation as in Figure 2

References

- [1] Henning E. Andersen and Olav Geil. Evaluation codes from order domain theory. *Finite Fields Appl.*, 14(1):92–123, 2008.
- [2] Gui Liang Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory*, 40(4):1003–1012, 1994.
- [3] Gui-Liang Feng and T. R. N. Rao. Improved geometric Goppa codes part I: Basic theory. *IEEE Trans. Inform. Theory*, 41(6):1678–1693, 1995.
- [4] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Des. Codes Cryptogr.*, 13(2):147–158, 1998.
- [5] Olav Geil and Ruud Pellikaan. On the structure of order domains. *Finite Fields Appl.*, 8(3):369–396, 2002.
- [6] Olav Geil and Christian Thommesen. On the Feng-Rao bound for generalized Hamming weights. In Marc P.C. Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 3857 of *Lecture Notes in Computer Science*, pages 295–306. Springer, 2006.
- [7] Petra Heijnen and Ruud Pellikaan. Generalized Hamming weights of q -ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.
- [8] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan. Algebraic geometry codes. In Vera S. Pless and William Cary Huffman, editors, *Handbook of Coding Theory*, volume 1, pages 871–961. Elsevier, Amsterdam, 1998.
- [9] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight. *IEICE Trans. Fundamentals*, E95-A(11):2067–2075, 2012.
- [10] Zihui Liu, Wende Chen, and Yuan Luo. The relative generalized Hamming weight of linear q -ary codes and their subcodes. *Des. Codes Cryptogr.*, 48(2):111–123, 2008.
- [11] Y. Luo, C. Mitropant, A.J.H. Vinck, and K. Chen. Some new characters on the wire-tap channel of type ii. *Information Theory, IEEE Transactions on*, 51(3):1222–1229, 2005.
- [12] Ryutaroh Matsumoto and Shinji Miura. On the Feng-Rao bound for the \mathcal{L} -construction of algebraic geometry codes. *IEICE Trans. Fundamentals*, E83-A(5):926–930, May 2000.
- [13] Shinji Miura. *Study of Error-Correcting Codes based on Algebraic Geometry*. PhD thesis, Univ. Tokyo, 1997. (in Japanese).
- [14] Ruud Pellikaan. On the efficient decoding of algebraic-geometric codes. In P. Camion, P. Charpin, and S. Harari, editors, *Eurocode '92 International Symposium on Coding Theory and Applications*, number 339 in CISM Courses and Lectures, pages 231–253. CISM International Centre for Mechanical Sciences, Springer, 1993.

- [15] G. Salazar, D. Dunn, and S. B. Graham. An improvement of the Feng-Rao bound on minimum distance. *Finite Fields Appl.*, 12:313–335, 2006.
- [16] V.K. Wei. Generalized hamming weights for linear codes. *Information Theory, IEEE Transactions on*, 37(5):1412–1418, 1991.